REMARKS

The claimed invention provides a system and method for setting up calls across a plurality of packet-switched networks interconnected to each other by network address translation (NAT) devices. The system comprises a plurality of call agents that communicate signaling messages according to some well-known protocol such as the Session Initiation Protocol (SIP). Each call agent sends and receives these messages to and from other call agents. The messages carry information used to set up a call session, including address information for media packets within the packet-switched networks. The address information defines a media path of the call.

In conventional systems, calls that traverse multiple NAT devices lose information about a preceding network at each NAT device. Therefore, in cases where a call is routed back to a network segment that the call has already traversed, it is not possible to re-connect the call directly to that preceding network segment. With the claimed invention, however, at least one of the messages communicated between the call agents includes address information that was sent to a preceding call agent involved in the set-up of the call. In some instances, the call agents "push" the address information (e.g., SIP session description information) of a preceding call agent that is involved in the call set-up a onto a stack structure to become part of a multipart attachment to the message. In other instances, the call agents "pop" address information off of the stack. Whether a given call agent pushes (i.e., adds) or pops (i.e., deletes) address information from the message is based at least in part on a set of predetermined rules consulted by the call agents.

Claim 20, which is directed to a call set-up system to set-up calls across a plurality of packet-switched networks connected to each other by NAT devices, stands finally rejected under 35 U.S.C. §103(a) as being obvious over the memo to Rosenberg entitled, "Supporting Intermediary Session Policies in SIP" in view of U.S. Pat. No. 7,574,735 ("Pirttimaa"). However,

neither reference, alone or in combination, teaches or suggests, "a plurality of call agents configured to... modify the at least one message by adding address information to, and deleting address information from, the at least one message," as claimed.

As acknowledged in the Office Action, Rosenberg fails to teach or suggest this limitation. However, Pirttimaa fails to remedy Rosenberg. Pirttimaa discloses a method for providing secure access to a network element, and also discloses passing SIP messages between elements. As seen in Figure 4, which is cited to support the rejection, a Proxy Call State Control Function (P-CSCF) receives a SIP message. However, rather than modify the SIP message, as claimed, the P-CSCF extracts the header of the message for a comparison to a set of security parameters stored in a local database (i.e., the SA database 30). Based on the result of the comparison, the P-CSCF generates a control signal to control whether a "Forwarding" function forwards the SIP message to the next element. *Pirttimaa*, col. 7, ll. 4-13.

In short, Prittimaa simply extracts a copy of the header information for comparison against predetermined data. Whatever address information is in the SIP message header, however, remains in the header. Further, there is no address information added to the SIP message header. Indeed, whatever comparison functions are performed in Pirttimaa do not teach, suggest, or even *hint* at modifying any of the SIP messages to add and delete address information, as claimed. In fact, Prittimaa is conspicuously silent about anything related to adding and deleting address information to/from the SIP header.

The fact that Pirttimaa does not teach or suggest modifying a SIP message to add and delete address information is not surprising because Pirttimaa is fundamentally concerned with the problem of secure access to a packet network. As explained in Pirttimaa,

> SIP messages between a UE and the P-CSCF 30 are integrity protected. This integrity protection also provides message origin authentication. The authenticated origin may be identified by any identity to which an integrity key has been explicitly or implicitly bound in the registration procedure. These identities include the IMPI and the registered IMPUs. However, a fraudulent user may use an integrity key bound to a registered IMPU to generate a correct

> message authentication code on a SIP message, e.g. SIP INVITE, but include the IMPU of another subscriber in the SIP message. This would lead to a number of threats, e.g. the S-CSCF 10 would then charge the session to the wrong IMPU.

Pirttimaa, col. 2, ll. 52-63. In other words, Pirttimaa discloses that a fraudulent user may include the IP Multimedia Public Identity (IMPU) of another user to generate a correct authentication in a SIP INVITE message, and recognizes that it would lead to a number of threats. Therefore, the solution disclosed in Figure 4 of Pirttimaa and its accompanying description merely compares addresses in order to determine whether any differences exist that would suggest a fraudulent user attack. Depending on the result, the message may be forwarded, but there is no modification of the message. Nor is there any need to modify the message in Pirttimaa.

Because both references alone fail to teach or suggest the above-cited limitation, the combination of the references also fails to teach or suggest this limitation. Accordingly, claim 20 and its dependent claims are note rendered obvious over Rosenberg in view of Pirttimaa.

Claim 38 is also independent, and stands rejected under §103(a) over the same references and for the same reasons as those stated above for claim 20. Claim 38 is a method claim that corresponds to claim 20 and contains similar language. Therefore, claim 38 is also non-obvious over the cited references.

The Office Action also indicates that claims 21-37 stand finally rejected under 35 U.S.C. §103(a) as being obvious over Rosenberg in view of Pirttimaa, and in further view of U.S. Pat. App. Pub. No. 2004/0114590 ("Harris"). However, these claims depend either directly or indirectly from claim 20, and thus, are also patentable over the cited art.

In light of the foregoing remarks, all claims are allowable over the cited art. Applicant

therefore respectfully requests that the Office issue a Notice of Allowance for all pending claims.

Respectfully submitted,
COATS & BENNETT, P.L.L.C.

Dated: January 27, 2012

Stephen A. Herrera
Registration No.: 47,642

1400 Crescent Green, Suite 300
Cary, NC 27518

Telephone: (919) 854-1844
Facsimile: (919) 854-2084